Department of Economic Security Information Technology Standards	Title: 1-38-0082 Wireless Policy	
Subject: This policy prohibits access to DES networks via unsecured wireless communication mechanisms.	***Effective Date:*** 04/27/05	***Revision:*** 1.1

1. Summary of Policy Changes

1.1. Original Implementation

2. Purpose

This policy prohibits access to DES networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy are approved for connectivity to the DES network. Unless there is a critical business/application need for use of wireless device, use must be restricted until technology and controls mature.

3. Scope and Background Information

This standard applies to all DES administrative entities, councils, divisions, administrations, programs and business partners. This policy covers all wireless data communication devices (e.g. personal computers, cellular phones, laptops, PDAs, etc.) connected to any of DES' internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to DES' networks do not fall under the scope of this policy.

DTS Telecommunications is responsible for providing a secure and reliable network to support the mission of DES. Under this broad responsibility, Telecommunications must promote agency-wide network standards (wired and wireless) to meet the networking requirements of all of DES constituencies and limit access to network connections which do not conform to generally accepted standard network protocols and security measures.

Due to the rapidly changing technology and application of this technology, additional guideline questions are bound to arise. This guideline, other relevant DES and GITA policies, and all applicable laws govern the use of electronic resources in the DES environment.

Background:

- Wireless technology allows for a greater mobility for electronic device users.
- Wireless technology, if not implemented and properly maintained, can create vulnerabilities to the DES enterprise and put DES data and equipment at risk.
- This technology is advancing at a rapid pace. Also advancing at a rapid pace are methods of breaching barriers established to protect wireless transmissions (i.e. ways of breaking encryption codes). Because of this, it is impossible to set specific standards for encryption methods that can be guaranteed to be effective in the future.
- DES is obligated by state and federal laws to protect confidential data.

4. Responsibilities

4.1. The DES Director, Deputy Directors, and Assistant Directors are responsible for enforcing this policy.

4.2. The Division of Technology Services is responsible for implementing this policy.

4.3. The DES Director, Deputy Directors, and Assistant Directors are responsible for identifying what constitutes a business need for implementing this technology for their respective areas.

4.4. DES employees and business partners have the responsibility to adhere to the guidelines set forth in this policy in order to ensure a secure networking environment and to protect DES data and equipment.

5. Definitions and Abbreviations

5.1. Definitions

5.1.1. **A**ccess **C**ontrol **L**ist**s** – (ACL's) – A method used in network devices such as routers to allow specific devices to access resources on private networks. These lists include specific devices allowed to attach; denying access to those devices not listed.

5.1.2. **Access Point** - An access point is a piece of wireless communications hardware, which creates a central point of wireless connectivity.

5.1.3. **Confidential Data/Information** – data whose loss, corruption or unauthorized disclosure would be a violation of Arizona Revised Statutes or federal mandates and regulations.

5.1.4. **Decrypt** – to change cipher text into plain text.

5.1.5. **Encryption** - is the conversion of data into a form (cipher text) that cannot be easily read by unauthorized people.

5.1.6. **Firewall** – is technology, hardware and/or software, used to restrict access to the network and/or IT resources.

5.1.7. IT Equipment includes:

5.1.7.1. **P**ersonal **C**omputers (PC), including desktops, and laptops.

5.1.7.2. Routers

5.1.7.3. **P**ersonal **D**igital **A**ssistants (PDAs) – Electronic hand-held devices commonly used for organizing (such as scheduling, contact information and task tracking).

5.1.7.4. Firewalls

5.1.7.5. Cell phones are included in this category for the purpose of this policy

5.1.8. **SSID** – **S**ervice **S**et **Id**entifier - A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters. An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

5.1.9. **User** – As used in this policy, User refers to a DES employee, contract employee, or other DES-authorized person who exchange electronic communications with DES.

5.1.10. **WAP - W**ireless **A**pplication **P**rotocol - defines a layered protocol stack that contains a session protocol (WSP), a transaction protocol (WTP), a security protocol (WTLS), and a datagram protocol (WDP). This stack isolates the application from the bearer when used as a transport service.

5.1.11. **WEP –** (Wired Equivalent Privacy) - Data encryption is defined by the 802.11 standard to prevent (i) access to the network by "intruders" using similar wireless LAN equipment and (ii) capture of wireless LAN traffic through eavesdropping. Access is denied by anyone who does not have an assigned key. This encryption standard has susceptibility to compromises.

5.1.12. **Wireless Communication** - is the ability to transmit data from point to point without the presence of a physical connection between the communicating devices. The key characteristic of wireless is the use of a multiple access radio system instead of wires to create the distribution/access network, whether or not point-to-point microwave is used as the backbone of the network.

5.1.13. **Wireless Infrastructure** – refers to the wireless access points, antennas, cabling, power and network hardware associated with the deployment of a wireless communications network.

5.1.14. **WLAN - W**ireless **L**ocal **A**rea **N**etwork - A local area network (LAN) that sends and receives data without a physical connection between individual nodes and a hub, such as through radio transmission.

5.2. **Abbreviations**

5.2.1. **CIO** – **C**hief **I**nformation **O**fficer

5.2.1. **CISO** – **C**hief **I**nformation **S**ecurity **O**fficer

5.2.1. **DES** – **D**epartment of **E**conomic **S**ecurity

5.2.1. **DTS** – **D**ivision of **T**echnology **S**ervices

5.2.1. **GITA** – **G**overnment **I**nformation **T**echnology **A**gency

5.2.1. **ISA** – Information Security Administration

5.2.1. **IT** – **I**nformation **T**echnology

5.2.1. **PC** – **P**ersonal **C**omputer

5.2.1. **PDA** – **P**ersonal **D**igital **A**ssistant

5.2.1. **SSID** – **S**ervice **S**et **Id**entifier

5.2.1. **WAP** – **W**ireless **A**pplication **P**rotocol

5.2.1. **WEP** – **W**ired **E**quivalent **P**rivacy

5.2.1. **WLAN** – **W**ireless **L**ocal **A**rea **N**etwork

6. Policy

6.1. DES employees and DES business partners will use the following guidelines when utilizing wireless technology in the DES computer network:

6.1.1. Authorization: All wireless implementations connecting to the DES network shall follow the following procedure for authorization of the implementation prior to deployment:

6.1.1.1. All implementations of wireless technology connecting to the DES network must be approved prior to the planning phase by the CIO (Chief Information Officer).

6.1.1.2. Prior to requesting approval of the CIO, the area requesting use of wireless technology must obtain their Assistant Director/Deputy Director approval of the business need for this technology.

6.1.1.3. SA and DTS technicians are to be included in the planning phase to provide technical guidance. Due diligence will be applied to ensure that the implementation is as secure as possible.

6.1.1.4. For each approved implementation, there will be named a party responsible for ensuring maintenance of the involved devices.

6.1.1.5. Access to wireless networks shall be requested by the user's supervisor or manager and documented on a "Request for Computer Access" form J-125.

6.1.2. Wireless Component Specifications and Use: All devices capable of wireless connectivity must meet the following specifications:

6.1.2.1. Wireless devices must be acquired through the standard network procurement processes.

6.1.2.2. All wireless devices connecting to the DES network must meet DTS specifications. Upgradeability of the device will be a factor in purchase decision making as new standards and updates are being released frequently and may need to be adopted.

6.1.2.3. Devices with wireless capability built-in will have the wireless capability disabled if compliance to6.1.1, 6.1.2, and 6.1.3 has not been achieved by the time of deployment. The disabling shall include eliminating the user's ability to enable wireless capability.

6.1.2.4. The service set identifier (SSID) shall be changed from the factory default setting on all clients and shall meet the following specifications:

- Unique
- Non-identifiable outside of DES
- Documented

6.1.2.5. The broadcast SSID feature shall be disabled, requiring wireless clients to scan for a specific access point.

6.1.2.6. The default cryptographic key shall be changed from the factory default setting.

6.1.2.7. Key management shall change cryptographic keys often.

6.1.2.8. Access point devices shall be managed via network management tools using SNMPv3 or higher. If network management is not being performed, SNMP shall be disabled.

6.1.2.9. Access points shall be manageable and configurable from a centralized location to facilitate software upgrades and centralized error and security reporting.

6.1.2.10. Access points shall be able to support wireless IDS functions, either as an adjunct to its client support or as a standalone passive monitor to detect rogue access points, detect unassociated clients and the detection of wireless scanning (war driving).

6.1.2.11. Access point devices shall be turned off during off-hours when not in use when possible.

6.1.2.12. Wireless access points and devices will be properly maintained to ensure that measures are taken to protect against the latest threats.

6.1.2.12.1. The responsible party of the device will frequently check for product vulnerabilities.

6.1.2.12.2. The responsible party will apply recommended fixes to the device to minimize vulnerability (such as patches, updating encryption methodology, virus protection software, etc.) within a prudent timeframe.

6.1.3. Security:

6.1.3.1.All logins to the wireless network must use an acceptable form of authentication (such as SecurId). Wireless network login methods other than SecurId must be approved by the CISO.

6.1.3.2. Access point insertion protection shall be accomplished by implementing 802.1x/EAP with RADIUS.

6.1.3.3.The following steps shall be taken for each wireless device (PDA, laptop, routers, etc.) to reduce risk:

6.1.3.3.1. Power-on passwords are to be implemented on each device to minimize the negative impact in the event the device is lost or stolen.

6.1.3.3.2. Provide physical protection for the wireless access points. (See Physical Security Policy). All infrastructure equipment is to be housed in a secure environment.

6.1.3.3.3. The following information shall be documented on each device in the event that it is lost or stolen:

6.1.3.3.3.1. Serial Number

6.1.3.3.3.2. MAC Address

6.1.3.3.3.3. DES Asset Tag Number (if applicable)

6.1.3.3.3.4. Make and Model

6.1.3.3.4. The user shall take responsible steps to prevent the loss, theft or preventable damage to the device and the data stored on it such as:

- The device shall not be left unattended if not secured (such as locked in a cabinet, behind a key-card access point, etc.)
- Do not leave the device unattended in plain site in a vehicle.
- Do not leave the device where it is exposed to the elements (such as in the trunk of the car during high temperatures).
- Do not loan the device to unauthorized individuals.
- Detect and eradicate viruses. Install virus protection and keep the signature files current.
- Backup handheld data regularly. Frequent backups can reduce loss of data and downtime when a Pocket PC is lost, stolen, wiped clean or damaged beyond repair.

6.1.3.3.5. Implement and properly configure firewalls on the mobile devices. Firewalls defend against port scans, unauthorized requests, unwanted peer-to-peer connections, denial of service floods, and other network-borne attacks.

6.1.3.3.6. The wireless device is not to be left unattended while attached to a computer.

6.1.3.3.7. All agencies must deploy wireless technologies with central administrative controls and awareness training.

6.1.3.3.8. Wireless transmissions shall be encrypted with secure methods. WEP is not considered the best method due to susceptibility to compromises. ISA and DTS will collaborate in determining the best method of encryption due to the fast pace this technology is changing at this time.

6.1.3.3.9. Key encryption strength should be a minimum of 128 bits. (Due to the rate of technology advances in this area, this minimum may change to accommodate industry enhancements.)

6.1.3.3.10. Connections shall be removed promptly when no longer required. Key network components shall be disabled or removed to prevent inadvertent reconnection.

6.1.3.3.11. Wireless sessions shall be routed to a centralized quarantine area in the network to utilize centralized firewalls, IDS/IPS, VPN and other security measures in place. All exceptions of this configuration must be approved by the CISO.

6.1.4. Wireless networks will be documented depicting:

6.1.4.1. SSID

6.1.4.2. Encryption method

6.1.4.3. Range of coverage (coverage power of access point)

6.1.4.4. Topography of the WLAN (location and description of involved devices including access points, antennas, cabling, and device names)

6.1.5. Policy Enforcement:

6.1.5.1. ISA will perform periodic audits of the DES network for unauthorized wireless devices as well as policy compliance.

6.1.5.2. DES employees are obligated to report any possible security incidents. Unauthorized or non-compliant wireless implementations constitute a security incident.

6.1.5.3. Any wireless connectivity to the DES network that does not meet the guidelines of this policy (including ISA security review approval) will be reported as a security incident and removed from the DES network until such time that ISA has deemed it as meeting DES security requirements.

6.1.5.4. As part of the corrective action for a founded security incident, disciplinary action may be taken toward the employee(s) responsible for implementing the non-compliant wireless connection.

7. Implications

7.1. This policy replaces all previous DES policy on the topics of wireless technology implementation and supports agency policies referencing the exchange of privileged and confidential information and enterprise security.

8. Implementation Strategy

8.1. This policy will be implemented upon publication.

8.2. Any existing wireless technology at the time of this publication must be documented and reviewed by ISA for policy compliance and security.

8.3. All devices that are currently deployed with wireless capability that do not meet 6.1.1, 6.1.2, 6.1.3 specifications shall have the wireless capability disabled and modified to not allow the user the ability to invoke wireless capability.

9. References

9.1. 1-38-0017 DES Client and Employee Information Transmission Policy

9.2. 1-38-0025 DES Access Control

10. Attachments

10.1. None

11. Associated Gita IT Standards or Policies

11.1. P100 – Information Technology

11.2. P700 – Enterprise Architecture

11.3. P710 – Network Architecture

11.4. P710 – S710 – Network Infrastructure

11.5. P800 Rev. 2.0 – IT Security

11.6. P800 – S830 Rev 1.0 – Network Security

12. Review Date

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.